23 March 2015

PRIVILEGED AND CONFIDENTIAL

The Secretary-General
Office of the Council of State
Phra Arthit Road, Phra Nakorn,
Bangkok 10200

Re: BSA Comments on Draft Personal Data Protection Act

Dear The Secretary-General

BSA | The Software Alliance (BSA)[1] welcomes this opportunity to provide comments concerning the Draft Personal Data Protection Act. We have closely monitored the development of the Draft Personal Data Protection Act and would like to offer our thanks for the transparent manner in which dialogues about the bill have been conducted.

BSA members recognize the importance of fostering trust and confidence in the online environment and are therefore deeply committed to protecting personal data across technologies and business models. Indeed, BSA members are at the forefront of data-driven innovation, including the development of cloud-based technologies that promote economic development and efficiency by enabling individuals and small businesses to leverage computing power that was once cost prohibitive.

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Altium, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, PTC, salesforce.com, Siemens PLM, Symantec, Tekla, The MathWorks, and Trend Micro.*

300 Beach Road
#25-08 The Concourse
Singapore 199555

P +65 6292 2072
F +65 6292 369
W bsa.org

Regional Representative Office
UEN: S97RF0005K

The continued development of these technologies requires a legal framework that is both clearly defined and reasonably flexible. Data protection laws must protect consumer privacy in a manner that does not create unnecessary barriers to the free flow of information that is the lifeblood of the 21st century economy. Although the version of the Draft Personal Data Protection Act currently before the Council of State is much improved from earlier versions, we provide these comments to flag for you several provisions that threaten to create unreasonable burdens and legal uncertainty for the technology sector.

Section 5: Definitions

"Personal Data" – The proposed definitions builds upon the concept of personal data used in the APEC Privacy Framework and the European Data Protection Directive, which capture any sort of information, regardless of form or content, whether that information relates to an identified or identifiable person. However, such a broad definition has been subject to much debate in Europe – for instance, some pieces of medical research have not been conducted in the EU as envisioned due to stringent prior consent requirements even when the data subjects could not be directly identified through information available to the personal data controller. Applying very stringent legal obligations to a broad range of data, regardless of its context and the actual potential for harm to the user, is likely to undermine Thailand's economic growth by chilling data driven innovation.

To avoid this, we suggest that the Council of State adopt a concept of personal data based on context, under which data would be deemed "personal data" only if the personal data controller can identify the individual to whom the data relates. Accordingly, we offer the proposed revision:

> *"Personal Data" means data regarding a person who can be identified whether directly or indirectly ~~from~~ ~~that~~ by the personal data controller.*

"Personal Data Controller" – Consistent with the APEC Privacy Framework, the proposed definition of "personal data controller" recognizes that the person or entity with the authority to make decisions regarding the management of personal information is best positioned to ensure its integrity. To ensure full consistency with the APEC Privacy Framework, we urge the Council of State to confirm that this provision will not implicate providers of cloud services who may host or process data at the direction of its users. To that end, we encourage the Council of State to add the following APEC Privacy Framework language to the definition:

> *"Personal Data Controller" means a person having the powers and duties to make decisions on the management of personal data, including the collection, use, and disclosure of personal data hereunder, but excludes a person or organization who performs such functions as instructed by another person or organization, or pursuant to contractual or legal obligations;*

Personal Data Protection Committee (Sections 7-18)

BSA strongly supports Thailand's effort to create a centralized personal data protection authority. Such a body can play an important role in educating consumers on how they can make informed choices regarding how their personal data is collected, used and stored. All computer users – consumers and businesses alike – should be educated on how to protect themselves from the growing number of online threats, including fraud and identity theft. The protection of privacy depends on informed consumers, responsible businesses and vigilant enforcement. This "shared responsibility" approach to privacy encourages consumers to be aware of privacy practices, to make choices about how their personal information will be used and to safeguard data under their control.

The Personal Data Protection Committee can also play an important role in overseeing the enforcement of the Personal Data Protection Act. With that said, we are concerned that several provisions may represent overly-broad delegations of authority. We note, for instance, that Sections 13(4) and 13(11) appear to grant the Committee with the authority to intervene in the data protection practices of a company, even in the absence of evidence that the company is failing to abide by the requirements of the Data Protection Act. Likewise, Section 16 authorizes the Committee to exercise its subpoena authority not only in the context of investigating a complaint, but also in furtherance of "any other matters" that the Committee deems appropriate. This unbounded delegation of authority is troubling. At a minimum, and consistent with principles of due process, we believe it is essential that the authorities under Sections 13(4), 13(11) and 16 be limited to circumstances in which the Committee has reasonable suspicion that a personal data collector has violated a provision of the Personal Data Protection Act.

The Committee's authority to promulgate "measures or guidelines" regarding data security practices under Section 13(3) should also be narrowed. The Committee should be directed, for instance, to ensure that any such measures are technologically neutral and that they not prescribe a "one-size-fits-all" approach to data security. Furthermore, guidelines issued by the Committee must not distort commonly accepted international standards pertaining to data security. To that end, the Committee should be authorized to issue guidelines only to the extent they are consistent with the globally accepted information security management system standards ISO/IEC 27001:2005 and ISO/IEC 17799:2005. These principles should also be incorporated into Sections 33-35, which similarly authorize the Committee to develop data protection codes of practice.

Collection of Personal Data (Sections 21-25)

Sections 21-25 create a framework under which personal data controllers must provide notice regarding the nature of their personal data collection efforts. BSA agrees that the requirement to notify the personal data owner before, or at the time of, the collection of personal information is generally reasonable. BSA members typically provide such notice through the use of easily accessible privacy policies that provide users with detailed information concerning the scope of data being collected and the purposes of its collection.

Of course, as Section 23 of the Draft Act recognizes, there are circumstances in which providing users with notification prior to the collection, use, or disclosure of personal information may not be reasonable or appropriate. Recognizing that, in addition to the enumerated circumstances in Article 23(1-6), the collection, use, or disclosure of certain personal information may be necessary in the course of legitimate and normal business activities, we urge the Council of State to consider including an additional exception to Section 23 to facilitate data collection in furtherance of the "legitimate interests" of data controllers. Such an exception is consistent with the European Union's approach to privacy in the Data Protection Directive (95/46/EC). This exception is not only important to ensure that reasonable business activities related to personal data can take place without undue burden or delay (*e.g.*, network and information security processing), it will also promote data protection and data minimization by reducing unintended incentives for the over-collection of personal data. In the absence of a "legitimate interests" exception, the Draft Act may inadvertently require personal data controllers to collect more data than is necessary for their business purposes in order to comply with the notification requirement. Maintaining a "legitimate interests" exception therefore promotes data minimization by ensuring that personal data controllers can collect only the information that is germane to their specific needs. We therefore urge the Council of State to add the following exception to Section 23:

> *(7) Data collected in advancement of the legitimate interests of the personal data controller.*

Section 24 raises similar concerns by requiring personal data controllers who collect data from third party sources to provide prompt notification to personal data owners whose information was implicated in such transactions. However, there are likely to be circumstances in which personal data collectors will obtain some form of personal information but lack the information necessary to make the required notification to the appropriate data owner. To avoid a scenario in which personal data collectors are required to obtain the personal contact information of each user whose data is included in a data transfer from a third party source, we recommend that the Council of State amend Section 24 as follows:

> *When collecting personal data from any other sources than directly from the personal data owner, a personal data controller must, to the extent feasible, notify the personal data owner promptly of the collection.*
> *Notification under Paragraph 1 is not necessary if the data is collected pursuant to an exemption under Section 23.*

Section 25 prohibits the collection of sensitive data without consent. While it is appropriate in some circumstances to impose more stringent requirements for the collection and use of particularly sensitive information, personal data collectors must have a clear understanding about when the heightened obligations are applicable. In this regard, we are concerned that the requirement to obtain consent prior to the collection of "data that affects the feelings of other persons or the public" will create tremendous uncertainty for personal data controllers.

Whether personal data will "affect the feelings" of the personal data owner is highly subjective determination – two individuals may react completely differently upon learning about the collection of a particular piece of information. It will therefore be impossible for personal data controllers to know when the Section 25 obligation is applicable. We urge the Council of State to remove this language from Section 25. Additionally, consistent with Section 23(4), we encourage the Council of State to expand the exceptions to Section 25 so that personal data controllers can freely collect information that has been "lawfully disclosed to the public." To accomplish these objectives, we recommend the following revisions:

> *No personal data related to race, ethnicity, political opinion, religious or philosophical belief, sexual behavior, criminal record, or health data, ~~or any other data that affects the feelings of other persons or the public,~~ as prescribed by the Committee, shall be collected without consent from the personal data owner or relevant persons, unless:*
>
> 1. *It is granted exemption under Section 23 (2), (3), (4), or (5); or*
> 2. *Any other cases as prescribed by ministerial regulations.*

Use of Personal Data (Section 26)

We remain deeply concerned that the Draft Act may be interpreted to impose on personal data collectors a separate duty to obtain consent prior to using data that was lawfully obtained with the knowledge of the personal data owner. In addition to the Section 22 obligation to provide notification to consumers in connection with the *collection* of personal data, Section 26 could potentially be interpreted to impose a separate obligation to obtain consent prior to any *use* of such data. Such a requirement is at odds with the APEC Privacy Framework and is, as a practical matter, untenable in the modern cloud environment.

The APEC Privacy Framework sets forth a reasonable system that ensures consumers receive notification about the type of data an online product or service will collect *and* how that data will be put to use. To fulfill this "Notice Principle," online service providers generally maintain privacy policies that users may review before any personal data is collected. The Notice Principle enables users to make informed decisions about whether they are comfortable with an online service's data collection practices. The APEC Privacy Framework further recognizes that the operator of an online service may use data it has collected from users to the extent such uses are consistent with the terms described in the notification.

If Section 26 of the Draft Act is interpreted as requiring operators of online services to obtain separate consent before making any use of personal data, in addition to the prior notification regarding the intended collection and use of such data, the Draft Act threatens to impose significant and unnecessary burdens on operators, the personal data controller, and the personal data owners. Such an interpretation of Section 26 is inconsistent with the carefully struck balance in the APEC Privacy Framework. Section 26 should be amended to clarify that

a personal data owner can provide consent for future uses of his or her data by agreeing to, or electing not to opt out of, an online service's privacy policy. Indeed, there are a wide range of mechanisms that enable users to control and consent to collection and use of their information, and some of the more robust opt-out mechanisms provide stronger protection for consumer privacy (with fewer disruptions for Internet users) than weaker opt-in mechanisms.

To ensure that Section 26 is interpreted consistently with the APEC Privacy Framework, we urge the Council of State to amend the provision accordingly:

> *Personal data controllers may use, transfer or disclose personal data only to fulfill the purposes of collection and other compatible or related purposes, as disclosed to the personal data owner pursuant to Section 22, except where:*
>
> 1. *The personal data owner has granted consent;*
> 2. *The use or disclosure is necessary to provide a service or product requested by the personal data owner;*
> 3. *The use or disclosure is necessary to fulfill a legal obligation; or*
> 4. *The personal data collected was collected pursuant to the exceptions under Section 23.*

International Transfers of Data (Section 27)

As it relates to cross-border data flows, Section 27 follows the "no transfer unless …" approach of the existing European Data Protection Directive. This approach has been heavily criticized because it is at odds with the vast increase in global data flows that has occurred in the 20 years since it was adopted.

Furthermore, the methods the EU law provides for transferring data, such as adequacy, model clauses and Binding Corporate Rules require companies to go through a rather onerous and long process, bringing these instruments out of reach for most companies.

In a world where cross-border data flows must be the rule rather than the exception, legal requirements need to be designed in a way that compliance is within reasonable reach for every entity treating personal information.

Therefore, we argue that the "accountability model," first established by the OECD and subsequently endorsed and integrated in many legal systems and privacy principles, including the APEC Cross-Border Privacy Rules (CBPR) and Canada's Personal Information Protection Act (which received an adequacy determination from the EU), would provide an approach to cross-border data governance that effectively provides the individual with protections and fosters streamlined, robust data flows. An accountability model requires that organizations that collect and use data are responsible for its protection and responsible use no matter where or by whom it is processed. It also requires that organizations transferring data must take appropriate steps to be sure that any obligations – in law, guidance or commitments made in privacy policies – will be met.

Therefore, we strongly encourage the Council of State to consider the benefits and the shortfalls of all options available before deciding on the final approach.

If the European model should be followed, account should be taken of additional exceptions that are being introduced as part of the ongoing legislative reform in the European Union. Those exceptions aim to make the system somewhat more flexible. For instance, recognition of standard contractual clauses in contracts between processors is being considered and would be a positive step towards making the system more flexible. Another example would be the increased flexibility for transfers between a corporate group or a group of enterprises engaged in a joint economic activity – the new proposal considers allowing the use of approved binding corporate rules for these groups' international transfers from the European Union to organizations within the same corporate group of undertakings or group of enterprises, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

Furthermore, a system of mutual recognition for standard contractual provisions and global corporate standards should be put in place in order to avoid multiple and potentially contradictory global requirements. In fact, the EU's Article 29 Working Party has recently published guidelines (*WP 226*) that will provide greater certainty for companies that transfer personal data outside of the Europe.

User Access to Data (Section 28)

Section 28 requires personal data controllers to provide personal data owners with access to the personal data that has been collected about them. BSA agrees that users should have an opportunity to review the scope of data collected about them. However, personal data controllers must have the discretion to reject such requests to the extent they pose legitimate threats to the security of a network. To that end, a personal data controller should be permitted to ignore requests that pertain to information collected or otherwise used in connection with reasonable network and information security practices. Without such an exception, compliance with Section 28 could create an elevated risk of data breaches. We therefore recommend the following revision:

> *Personal data owners have the right to request access to their personal data under the responsibility of the personal data controller, except in the following cases:*
>
> 1. *It is in conflict with, or contrary to, the provision of other laws or court orders;*
> 2. *It affects the security of the Kingdom;*
> 3. *It affects the country's economy and commerce;*
> 4. *It affects the investigation or interrogation by the competent officers under the law or court proceeding; ~~or~~*

5. *It is for the protection of the personal data owner or the rights and liberties of other persons~~.~~; or*
6. *It would undermine reasonable network and information security efforts.*

Accuracy of Personal Data (Section 30)

Section 30 requires personal data controllers to maintain the accuracy of personal data that they have collected. Although online service providers have a strong business interest in ensuring that the data they have collected remains accurate, their ability to do so is often constrained. Because personal data controllers can only update personal information when such information is made available to them, we urge the Council of State to amend Section 30 as follows:

> *The personal data controller shall, to the extent reasonable, ensure that the personal data is accurate, updated, complete, and not misleading, unless otherwise stipulated by law.*

Personal Data Controller Duties – Data Breach Notification (Section 31)

BSA supports the creation of a personal data breach notification system applicable to all businesses and organizations. Appropriately crafted data breach provisions incentivize the adoption of robust data security practices and enable individuals to take action to protect themselves in the event their data is compromised. When developing data breach notification provisions, it is critical to recognize that not all data breaches represent equal threats. In many instances, data breaches pose no actual risks to the individuals whose data was compromised.

To ensure that consumers are not inundated with notices regarding immaterial data breaches, the notification obligation should be triggered only in circumstances that pose credible risks of harm to users. For instance, the obligation to provide notice should not apply to instances in which the breached data is unusable, unreadable or indecipherable to an unauthorized third party through practices or methods (e.g., encryption) that are widely accepted as effective industry practices or industry standards. Finally, to ensure users receive meaningful notification in the event of a breach, it is critical that data controllers are afforded adequate time to perform a thorough risk assessment to determine the scope of the security risk and prevent further disclosures. It is therefore counterproductive to include within the data breach provision a fixed deadline for providing notification.

Based on the foregoing, we recommend the following revisions to Section 31(4):

> *To notify the personal data owner of a breach of personal data that creates a significant risk of harm, without unreasonable delay, and the remedial plan for the damage due to the breach of personal data.*

In instances where a breach of personal data creates a significant risk of harm for more than, 10,000 people the data controller shall also notify the Committee. In no instance shall a personal data controller be required to provide notification if the compromised data was stored in a manner that renders it unusable, unreadable or indecipherable to an unauthorized third party through practices or methods that are widely accepted as effective industry practices or industry standards.

Civil Liability (Section 42)

To ensure that data controller are adequately motivated to implement reasonable data security measures, it is appropriate to impose civil liability for violations of this Act. When designing a civil liability framework, however, it is critical to acknowledge that even the most robust data security measures may in some instances be undermined by determined criminal hackers. It would therefore be inappropriate to expose a data controller to liability in the absence of evidence demonstrating that he or she violated a provision of this Act, which is intended to establish legal norms for the collection, use and protection of personal information. We therefore recommend that the Council of State revise Section 42 as follows:

Where a personal data controller's failure to adhere to the obligations set forth in this Act is the proximate cause of direct and actual damages to a personal data owner, the personal data controller shall compensate the personal data owner in an amount equal to the direct and actual damages.

A personal data operator shall not be liable for any damages that arise from:

1. *a force majeure event;*
2. *performance under an order of the government or a government official;*
3. *an action, or omission, of related persons or other persons; or*
4. *completion of personal data protection practice codes set out by that person.*

Criminal Liability (Sections 43-46)

The threat of criminal liability is appropriate only in instances involving grave and intentional violations of law. We note with tremendous concern that the criminal liability provisions of the Draft Act, as currently drafted, may apply in circumstances involving minor, or even accidental, violations of law. For instance, Section 44 criminalizes any violation of the obligations set out in Sections 22, 24, 25, 26, 27, 30, 31, or 32. Although a technical violation of Section 22 might occur if the webpage on which a data controller's privacy policy were to temporarily go down, thus preventing the data controller from providing adequate notification to users of the site, imposing criminal liability in such a scenario would be deeply troubling. To ensure that mere technical

violations do not create a risk of criminal liability, we urge the Council of State to amend Section 44 accordingly:

> *Any personal data controller ~~violating or failing to comply with~~ that knowingly and intentionally violates the first paragraph of Section 22, Section 24, Section 25, Section 26, Section 27, Section 30, Section 31, or Section 32 for purposes of personal financial gain or other benefit or with the intention of harming a personal data owner shall be subject to imprisonment for a term not exceeding six months, or a fine not exceeding Baht 300,000 or both.*
>
> *~~Any person who performs action under the first paragraph to seek unlawful benefits for that person or other person or to the detriment of other persons shall be subject to imprisonment for a term not exceeding two years or a fine not exceeding Baht 2,000,000, or both.~~*

Perhaps more alarmingly, proposed Section 45 would criminalize behavior that is explicitly permitted by other provisions of the Draft Act. For example, whereas Section 26 permits use or disclosure of personal data with the "consent" of the personal data owner, Section 45(6) threatens to impose criminal liability unless the data controller obtains "*written* consent." As discussed above in relation to Section 26, requiring data controllers to separately obtain consent for each use or transfer of personal data is entirely unrealistic in the modern Internet ecosystem. The very existence of cloud-based technologies and e-commerce relies on the ability of service providers to seamlessly transfer data to provide consumers with the products and services they demand. For example, if a company uses an online payroll vendor, it must disclose personal data about its employees to the payroll vendor in order to ensure they are paid in a timely manner. This is but one example of the hundreds, if not thousands, of uses of an individual's personal information that now occur daily. In view of this reality, we urge the Council of State to amend both Section 26 and Section 45 to ensure that data collectors may lawfully make use of data (including transfers and/or disclosures of such data) to the extent the data was collected with the knowledge of the personal data owner.

Conclusion

BSA appreciates the attempt to uphold the rights to privacy and trusts that properly drafted legislation would lead to effective enforcement. BSA, therefore, humbly requests that serious consideration be given to the above comments in order bring about the best solution for all the sectors involved. We remain open to further discussion with you at any time. Please feel free to contact **Ms. Varunee Ratchatapattanakul, BSA's Thailand Representative, at varuneer@bsa.org or +668-1840-0591** with any questions or comments which you might have.

Thank you for your time and consideration.

Yours sincerely,

Boon Poh Mok
Director, Policy, APAC
BSA | The Software Alliance

Cc:

1. H.E. Dr. Vishnu Khruangam, Deputy Prime Minister of Thailand
2. Mrs. Surangkana Wayuparb, Executive Director and CEO of The Electronic Transactions Development Agency (Public Organization)